# Vendor Risk Management Program

ClearPath Pharmacy: GRC Portfolio

| Document information | Details |
|---|---|
| Organization | ClearPath Pharmacy: Specialty Pharmacy Services |
| Document title | Third-Party / Vendor Risk Management Program |
| Document ID | CP-TPRM-001 |
| Classification | Confidential: Internal Use Only |
| Version | 1.0 |
| Effective date | May 18, 2026 |
| Next review date | May 18, 2027 |
| Prepared by | Information Security & Compliance Department |
| Approved by | Information Security Steering Committee |

**Governing references:** General TPRM practice with NIST SP 800-161 (supply chain risk) as the backbone, and HIPAA Business Associate requirements as the healthcare layer. This program adds the operational vendor-risk layer to ClearPath's existing GRC portfolio.

## 1. Program Purpose, Scope, and Governance

This program governs how ClearPath identifies, assesses, contracts with, monitors, and offboards third-party vendors, with the highest scrutiny on any vendor that can access protected health information. The Information Security & Compliance Department owns the program; the Information Security Steering Committee accepts residual vendor risk.

- Scope: all vendors, service providers, and technology partners with access to ClearPath systems, facilities, or data.
- Ownership: a named program owner maintains the vendor inventory, register, and BAA tracking.

## 2. Vendor Inventory and Classification

Every vendor is tiered by criticality and by data access. The single most important question is whether the vendor can touch PHI. PHI-handling vendors are always the highest tier.

| Tier | Criticality | Data access | Examples |
|---|---|---|---|
| Tier 1 (Critical) | Core operations or PHI | Creates, receives, maintains, or transmits PHI | AOP analytics vendor, pharmacy management system, cloud hosting of ePHI |
| Tier 2 (Important) | Significant but not PHI-bearing | Limited or no PHI; sensitive business data | Billing analytics on de-identified data, IT support |
| Tier 3 (Standard) | Low impact | No PHI; non-sensitive data | Office supplies, marketing tools on public data |

## 3. Due Diligence and Risk Assessment Process

1. Before onboarding, review the vendor's security posture, certifications (SOC 2, HITRUST, ISO 27001), financial stability, and subprocessor chain.
2. Require the Vendor Risk Assessment Questionnaire (Appendix A) for all Tier 1 and Tier 2 vendors.
3. Assign a risk rating and document it in the Vendor Risk Register (Appendix B).
4. For any vendor that will touch PHI, confirm a signed BAA is in place before access is granted.

## 4. Contractual Controls

| Tier | Required contractual controls |
|---|---|
| Tier 1 | Signed BAA (mandatory before access), security and breach-notification clauses, audit rights, subprocessor disclosure, data return/destruction terms |
| Tier 2 | Security and confidentiality clauses, breach notification, data handling terms; BAA if any PHI is involved |
| Tier 3 | Standard confidentiality and acceptable-use terms |

**HIPAA hook:** Any vendor that creates, receives, maintains, or transmits PHI is a Business Associate and requires a signed Business Associate Agreement before access. BAA tracking is a core, audited requirement of this program, not an afterthought.

## 5. Ongoing Monitoring and Reassessment

| Tier | Reassessment cadence | Trigger events for immediate re-review |
|---|---|---|
| Tier 1 | At least annually | Vendor breach, BAA lapse, ownership change, major service change |
| Tier 2 | Every 18 to 24 months | Security incident, scope change adding data access |
| Tier 3 | At renewal | Any new data access or incident |

## 6. Offboarding

- ☐ Revoke all vendor access to systems, facilities, and accounts.
- ☐ Confirm secure return or certified destruction of ClearPath data, including PHI.
- ☐ Close out the BAA and document surviving obligations (for example, retention and confidentiality).
- ☐ Update the vendor inventory and register to reflect the offboarded status.

## Appendix A: Vendor Risk Assessment Questionnaire (template)

Issue to all Tier 1 and Tier 2 vendors before onboarding and at reassessment.

| # | Question | Response |
|---|---|---|
| 1 | Does your service create, receive, maintain, or transmit PHI for ClearPath? | Yes / No |
| 2 | Will you sign ClearPath's Business Associate Agreement? | Yes / No / N/A |
| 3 | What security certifications do you hold (SOC 2, HITRUST, ISO 27001)? | |
| 4 | How is data encrypted in transit and at rest? | |
| 5 | List subprocessors and their data access. | |
| 6 | What is your breach notification commitment and timeline? | |
| 7 | Describe your access control and workforce security practices. | |

| # | Question | Response |
|---|---|---|
| 8 | How is ClearPath data returned or destroyed at contract end? | |

## Appendix B: Vendor Risk Register (template)

| Vendor | Service | Data accessed | PHI ? | Tier | BAA status | Risk rating | Next review |
|---|---|---|---|---|---|---|---|
| MedSignal Analytics | AOP predictive tool | PHI | Yes | 1 | Signed | Medium | May 2027 |
| [vendor] | [service] | [data] | Y/N | 1-3 | Signed / Pending / N/A | H/M/L | [date] |

Columns: vendor, service, data accessed, PHI yes/no, tier, BAA status, last assessed, risk rating, owner, next review. Keep the register as the single source of truth for vendor risk and BAA coverage.